EXHIBIT C-11
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 11 ('661 Patent)	U.S. Patent No. 5,341,423 to Nossen ("Nossen")
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:23-39 – "Many techniques have been advanced to make interception of communications difficult. For example, spread-spectrum techniques such as frequency hopping and direct sequence spreading reduce the average transmitted power in a given bandwidth to make interception difficult. The phase of a carrier can be randomized as described in U.S. patent application Ser. No. 724,309 filed Apr. 12, 1985, now U.S. Pat. No. 4,652,838 in the name of Nossen, to reduce the detected power density. It is often desirable to combine two or more communication techniques in order to further increase the difficulty of receiving a transmitted signal or of decoding the information contained therein. Thus, it is advantageous to have many techniques for preventing the reception of transmissions, for preventing the decoding of the information contained therein if the transmissions are received, or both." 2:58-64 – "FIG. 1 is a block diagram of a portion of a communication system according to the invention. The communication system includes a master station or master transmitter-receiver designated generally as 10, one or more mobile stations, one of which is illustrated as station 30, and one or more masking or decoy stations, one of which is illustrated as station 50."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:24-34 – "Master station 10 as illustrated in FIG. 1 includes an antenna 12 and a frequency diplexer 14. Diplexer 14 couples signals received by antenna 12 at frequency F_2 to a receiver (Rx) 16, and accepts signals at frequency F_1 from a transmitter (Tx) 18 for application to antenna 12. The signals received at frequency F_2 are processed and demodulated in receiver 16, as for example by downconverting to an IF frequency, and the signals so processed are applied over a conductor 17 to a masking signal cancelling arrangement illustrated as a block 20 to unmask the mobile station data signal."
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of	Figure 2.

Exhibit C-11 (Nossen)

said operation;	
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	3:29-47 – "The signals received at frequency F_2 are processed and demodulated in receiver 16, as for example by downconverting to an IF frequency, and the signals so processed are applied over a conductor 17 to a masking signal cancelling arrangement illustrated as a block 20 to unmask the mobile station data signal. The masked and unmasked data signals are applied from cancelling arrangement 20 by way of conductor 21 to a processing block 22 which demodulates the unmasked signal originating from mobile station 30, and which also notes the relative amplitudes of the data and masking signals, and generates instructions for transmission to mobile station 30 and masking station 50 for control of the amplitudes and possibly the phases their signals. Processor 22 also receives data at a data I/O port from conductor 23 for transmission to the mobile stations, processes it for transmission and applies it over a conductor 25 to a transmitter 18."
(d) a noise production system for introducing noise into said measurement of said power consumption.	4:25-28 – "The signal transmitted by masking or decoy station 50 is modulated by an unmodulated pseudorandom sequence (i.e., one without periodic phase inversions due to data content)." 4:34-44 – "The chip rates and chip clock phases of the pseudorandom sequences of mobile station 30 and decoy station 50 are monitored at station 10, and instructions are transmitted at frequency F_1 from base station 10 and received by mobile station 30, decoy station 50, or both, for control of the chip rates to make the chip rates of the pseudorandom sequences equal. The frequency equality of chip rates, together with the equal transmitting frequencies, makes it impossible for an unauthorized signal interceptor to distinguish the signal of the mobile station from that of the decoy station."

Claim 29 ('661 Patent)	U.S. Patent No. 5,341,423 to Nossen
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption,	1:23-39 – "Many techniques have been advanced to make interception of communications difficult. For example, spread-spectrum techniques such as frequency hopping and direct sequence spreading reduce the average transmitted power in a given bandwidth to make interception difficult. The phase of a carrier can be randomized as described in U.S. patent application Ser. No. 724,309 filed Apr. 12, 1985, now U.S. Pat. No. 4,652,838 in the name of Nossen, to reduce the detected power density. It is often desirable to combine two or more communication techniques in order to further increase the difficulty of receiving a transmitted signal or of decoding the information contained therein. Thus, it is advantageous to have many

Exhibit C-11 (Nossen)

comprising:	techniques for preventing the reception of transmissions, for preventing the decoding of the information contained therein if the transmissions are received, or both." 2:58-64 – "FIG. 1 is a block diagram of a portion of a communication system according to the invention. The communication system includes a master station or master transmitter-receiver designated generally as 10, one or more mobile stations, one of which is illustrated as station 30, and one or more masking or decoy stations, one of which is illustrated as station 50."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	Figure 2.
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:24-34 – "Master station 10 as illustrated in FIG. 1 includes an antenna 12 and a frequency diplexer 14. Diplexer 14 couples signals received by antenna 12 at frequency F_2 to a receiver (Rx) 16, and accepts signals at frequency F_1 from a transmitter (Tx) 18 for application to antenna 12. The signals received at frequency F_2 are processed and demodulated in receiver 16, as for example by downconverting to an IF frequency, and the signals so processed are applied over a conductor 17 to a masking signal cancelling arrangement illustrated as a block 20 to unmask the mobile station data signal."
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	4:25-28 – "The signal transmitted by masking or decoy station 50 is modulated by an unmodulated pseudorandom sequence (i.e., one without periodic phase inversions due to data content)." 4:34-44 – "The chip rates and chip clock phases of the pseudorandom sequences of mobile station 30 and decoy station 50 are monitored at station 10, and instructions are transmitted at frequency F_1 from base station 10 and received by mobile station 30, decoy station 50, or both, for control of the chip rates to make the chip rates of the pseudorandom sequences equal. The frequency equality of chip rates, together with the equal transmitting frequencies, makes it impossible for an unauthorized signal interceptor to distinguish the signal of the mobile station from that of the decoy station." 3:29-34 – "The signals received at frequency F_2 are processed and demodulated in receiver 16, as for example by downconverting to an IF frequency, and the signals so processed are applied over a

	conductor 17 to a masking signal cancelling arrangement illustrated as a block 20 to unmask the mobile station data signal."
(d) outputting said cryptographically processed quantity to a recipient thereof.	3:43-47 – "Processor 22 also receives data at a data I/O port from conductor 23 for transmission to the mobile stations, processes it for transmission and applies it over a conductor 25 to a transmitter 18."